

§ 1016.3 Definitions.

(a) *Access authorization or security clearance.* An administrative determination by the DOE that an individual who is either a DOE employee, applicant for employment, consultant, assignee, other Federal department or agency employee (and other persons who may be designated by the Secretary of Energy), or a DOE contractor or subcontractor employee and an access permittee is eligible for access to Restricted Data. Access authorizations or security clearances granted by DOE are designated as "Q," "Q(X)," "L," "L(X)," "Top Secret," or "Secret." For the purpose of this chapter only "Q," "Q(X)," "L," and "L(X)" access authorizations or clearances will be defined.

(1) "Q" access authorizations or clearances are based upon full field investigations conducted by the Federal Bureau of Investigation, Office of Personnel Management, or another Government agency which conducts personnel security investigations. They permit an individual to have access, on a "need to know" basis, to Top Secret, Secret, and Confidential Restricted Data, Formerly Restricted Data, National Security Information, or special nuclear material in Category I or II quantities as required in the performance of duties.

(2) "Q(X)" access authorizations or clearances are based upon the same full field investigations as described in § 1016.3(a)(1), above. When "Q" access authorizations or clearances are granted to access permittees they are identified as "Q(X)" access authorizations or clearances and authorize access only to the type of Secret Restricted Data as specified in the permit and consistent with appendix A, 10 CFR part 725, "Categories of Restricted Data Available."

(3) "L" access authorizations or clearances are based upon National Agency Checks and Inquiries (NACI) for Federal employees, or National Agency Checks (NAC) for non-Federal employees, conducted by the Office of Personnel Management. They permit an individual to have access, on a "need to know" basis, to Confidential Restricted Data, Secret and Confidential Formerly Restricted Data, or Secret and Confidential National Security

Information, required in the performance of duties, provided such information is not designated "CRYPTO" (classified cryptographic information), other classified communications security ("COMSEC") information, or intelligence information.

(4) "L(X)" access authorizations or clearances are based upon the same National Agency Checks as described in paragraph (a)(3), of this section. When "L" access authorizations or clearances are granted to access permittees, they are identified as "L(X)" access authorizations or clearances and authorize access only to the type of Confidential Restricted Data as specified in the permit and consistent with appendix A, 10 CFR part 725, "Categories of Restricted Data Available."

(b) *Act.* The Atomic Energy Act of 1954 (68 Stat. 919) as amended.

(c) *Authorized classifier.* An individual authorized in writing by appropriate DOE authority to classify, declassify, or downgrade the classification of information, work, projects, documents, and materials.

(d) *Classified mail address.* A mail address established for each access permittee approved by the DOE to which all Restricted Data for the permittee is to be sent.

(e) *Classified matter.* Documents and material containing classified information.

(f) *Combination lock.* A built-in combination lock on a security container which is of tempered steel alloy hard plate, at least ¼" in thickness and Rockwell hardness of C-63 to C-65, of sufficient size and so located as to sufficiently impede access to the locking mechanism by drilling of the lock or container.

(g) *DOE.* The United States Department of Energy or its duly authorized representatives.

(h) *Document.* Any piece of recorded information regardless of its physical form or characteristics.

(i) *Formerly Restricted Data.* Classified information jointly determined by the DOE and the Department of Defense to be related primarily to the military utilization of atomic weapons and removed by the DOE from the Restricted Data category pursuant to section

142(d) of the Atomic Energy Act of 1954, as amended.

(j) *Infraction.* An act or omission involving failure to comply with DOE safeguards and security orders or directives, and may include a violation of law.

(k) *Intrusion alarm.* A tamper-indicating electrical, electro-mechanical, electro-optical, electronic or similar device which will detect unauthorized intrusion by an individual into a building or security area, and alert protective personnel by means of actuated visible and audible signals.

(l) *Material.* A chemical substance without regard to form; fabricated or processed item; or assembly, machinery, or equipment.

(m) *Matter.* Documents or material.

(n) *National Security.* The national defense and foreign relations of the United States.

(o) *National Security Information.* Information that has been determined pursuant to Executive Order 12356 of April 2, 1982, "National Security Information" or any predecessor order to require protection against unauthorized disclosure and that is so designated.

(p) *"Need to know."* A determination by persons having responsibility for classified information or matter, that a proposed recipient's access to such classified information or matter is necessary in the performance of official, contractual, or access permit duties of employment under cognizance of the DOE.

(q) *Permittee.* The holder of an Access Permit issued pursuant to the regulations set forth in 10 CFR part 725, "Permits For Access to Restricted Data."

(r) *Person.* Any individual, corporation, partnership, firm, association, trust, estate, public or private institution, group, Government agency other than DOE, any State or any political subdivision of, or any political entity within a State, or other entity; and any legal successor, representative, agency, or agency of the foregoing.

(s) *Protective personnel.* Guards or watchmen or other persons designated responsibility for the protection of classified matter.

(t) *Restricted Data.* All data concerning design, manufacture, or utilization of atomic weapons; the production of

special nuclear material; or the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the Restricted Data category pursuant to section 142 of the Act.

(u) *Security area.* A physically defined space containing classified matter and subject to physical protection and personnel access controls.

(v) *Security clearance.* See access authorization.

(w) *Security facility.* Any facility, including an access permittee, which has been approved by the DOE for using, processing, storing, reproducing, transmitting, or handling classified matter.

(x) *Security facility approval.* A determination by the DOE that a facility, including an access permittee, is eligible to use, process, store, reproduce, transmit, or handle classified matter.

(y) *Security Plan.* A written plan by the access permittee, and submitted to the DOE for approval, which outlines the permittee's proposed security procedures and controls for the protection of Restricted Data and which includes a floor plan of the area in which the matter is to be used, processed, stored, reproduced, transmitted, or handled.

(z) *Security survey.* An onsite examination by a DOE representative of all devices, equipment, and procedures employed at a security facility to safeguard classified matter.

§ 1016.4 Communications.

Communications concerning rule-making, i.e., petition to change part 1016, should be addressed to the Assistant Secretary for Defense Programs (DP-1), U.S. Department of Energy, Washington, D.C. 20545. All other communications concerning the regulations in this part should be addressed to U.S. Department of Energy Operations Offices as listed in appendix B of 10 CFR part 725, administering access permits for the geographical area.

§ 1016.5 Submission of procedures by access permit holder.

No access permit holder shall have access to Restricted Data until he shall have submitted to the DOE a written statement of his procedures for the safeguarding of Restricted Data and for